JOURNAL OF ALGEBRA 53, 40–57 (1978)

A Characterization of $SL(2, p^n)$, $p \geqslant 5$

CHAT-YIN HO

Universidade de Brasília, Departamento de Matemática, IE 70.000, Brasília, DF, Brasil

Communicated by Walter Feit

Received September 12, 1977

DEDICATED TO THE MEMORY OF RICHARD BRAUER

1. INTRODUCTION AND NOTATION

If M is a faithful irreducible G-module, where M is a finite dimensional vector space over the finite field of p elements and G is a finite group, we can ask whether any p-element of G has a quadratic minimal polynomial. The study of this question turns out to be of fundamental importance in a variety of problems, especially in the study of finite simple groups. If $p = 2$, then obviously any element x of order 2 satisfies the polynomial $X^2 - 1 = (X - 1)^2$, as V is faithful, this must be its minimal polynomial. We see then the question is meaningful only when p is odd. In 1970, Thompson solved this problem for the case $p \geqslant 5$ in [13] and the current situation about this question can be found in [10]. In treating this question, the 2-dimensional special linear group $\mathrm{SL}(2, p^n)$, where p is an odd prime, plays an important role.

If $G = \mathrm{SL}(2, p^n)$ acting on a natural 2-dimensional vector space M over the field with p^n elements, then a nontrivial p-element has a quadratic minimal polynomial. Furthermore for any two nontrivial p-elements σ, τ of G, $|M(\sigma - 1)| = |M(\tau - 1)|$. The objective of this paper is to prove the following results.

THEOREM A. *Let G be a finite group and let M be a finite dimensional vector space over the finite field with p elements, where p is a prime bigger than or equal to 5. Suppose G is generated by its elements of order p and M is a faithful G-module. If for every nontrivial element σ of order p in G we have $M(\sigma - 1)^2 = 0$, then $G = O_p(G) * S_1 * \cdots * S_n$, where $S_i \cong \mathrm{SL}(2, p^{a_i})$ for some positive integer a_i if $S_i \neq 1$ for $i = 1, \ldots, n$. Furthermore the nilpotent class of $O_p(G)$ is at most 2 and the exponent of $O_p(G)$ is at most p.*

THEOREM B. *If in addition to the conditions of Theorem A we assume that*

0021-8693/78/0531–0040$02.00/0

$|M(\sigma - 1)| = |M(\tau - 1)|$ *for any two nontrivial elements* σ, τ *of order* p *in* G, *then one of the following holds.*

(1) G *is an elementary abelian* p*-group.*

(2) $G \cong \mathrm{SL}(2, p^a)$ *for some positive integer* a.

Let V be a vector space over the field $\mathrm{GF}(p)$ of p elements, p a prime. We write $\dim V$ to mean $\dim_{GF(p)} V$. Let S be a set of linear transformations of V. We set $Q(S, V) = \{\sigma \in S \mid \sigma \neq 1 \text{ and } V(\sigma - 1)^2 = 0\}$, $V_S = \{v \in V \mid vs = v \text{ for all } s \in S\}$ and $V^S = \{v(s - 1) \mid v \in V \text{ and } s \in S\}$. For $\sigma \in Q(S, V)$, let $d(\sigma) = \dim V^\sigma$. If $Q(S, V) \neq \varnothing$, we set $d(S, V) = \min\{d(\sigma) \mid \sigma \in Q(S, V)\}$ and $Q_d(S, V) = \{\sigma \in Q(S, V) \mid d(\sigma) = d(V, S)\}$.

For $\sigma \in Q_d(S, V)$, let $E(\sigma) = \{\tau \in Q(S, V) \mid M^\sigma = M^\tau \text{ and } M_\tau = M_\sigma\} \cup \{1\}$ and $U(\sigma) = \{\tau \in S \mid \tau \text{ stabilizes the chain } V \geqslant V_\sigma \geqslant V^\sigma \geqslant 0\}$. We also set $\Sigma(S, V) = \{E \mid E = E(\sigma) \text{ for some } \sigma \in Q_d(S, V)\}$.

In discussing matrices we adopt the following abused convention. The zero and the identity matrices of various degree are denoted by 0 and I. For a square matrix α, $R(\alpha)$ denote the matrix $\left(\begin{smallmatrix} I & \alpha \\ 0 & I \end{smallmatrix}\right)$ and $R'(\alpha)$ denotes the matrix $\left(\begin{smallmatrix} I & 0 \\ \alpha & I \end{smallmatrix}\right)$. All groups considered in this paper will be of finite order. For any group X, we define $X_1 = X$ and $X_i = [X_{i-1}, X]$ for $i > 2$. X is nilpotent if $X_k = 1$ for some k. In this case the smallest positive integer c such that $X_{c+1} = 1$ is called the nilpotent class of X and is denoted by $\mathrm{cl}(X)$. Most of our notation is standard and can be found in [4]. We point out that Theorem B is a generalization of Theorem 1 of [12] in the case $p \geqslant 5$.

The organization of the paper is as follows. In Section 2 we reproduce and generalize some unpublished important results in [13]. Section 3 treats the structure of p-subgroups. In Section 4 the proofs of Theorems A and B are presented. Also several remarks in the case $p = 3$ are included in this final section.

2. p-Nonstable Representation

In this section we assume that p is a prime, M a vector space over the finite field $\mathrm{GF}(p)$ with p elements and G, a group, acts faithfully on M such that $Q(G, M) \neq \varnothing$. For any σ, $\tau \in Q(G, M)$. let $\Delta(\sigma, \tau) = (\sigma - 1)(\tau - 1) + (\tau - 1)(\sigma - 1)$. We take this opportunity to reproduce and generalize some well known results of [13]. Let $Q = Q(G, M)$, $d = d(G, M)$, $Q_d = Q_d(G, M)$ and $\Sigma = \Sigma(G, M)$.

Lemma 2.1. *Let* $\sigma, \tau \in Q$. *Then the following statements are valid.*

(a) $\Delta(\sigma, \tau)$ *commutes with* σ *and* τ.

(b) $H = \langle \sigma, \tau \rangle$ *is a* p*-group if and only if* $\Delta(\sigma, \tau)$ *is nilpotent.*

Proof. The proof presented in the proof of Lemma 3.2 of [12] applies here.

LEMMA 2.2. *Let $\sigma \in Q_d$. Then $E(\sigma)$ is an elementary abelian p-group and $E(\sigma) = E(\tau)$ for any $\tau \in E(\sigma)\backslash\{1\}$. If $\sigma, \gamma \in Q_d$, then either $E(\sigma) = E(\gamma)$ or $E(\sigma) \cap E(\gamma) = 1$.*

Proof. Let $\rho, \tau \in E(\sigma)\backslash\{1\}$. Since $M^\tau = M^\sigma = M^\rho \leqslant M_\sigma = M_\tau = M_\rho$, $\rho\tau - 1 = (\rho - 1)(\tau - 1) + (\rho - 1) + (\tau - 1) = (\rho - 1) + (\tau - 1)$. Thus $M^{\rho\tau} \leqslant M^\rho$ and $M(\rho\tau - 1)^2 = 0$. Hence $\rho\tau = 1$ or $\rho\tau \in Q$. Suppose $\rho\tau \in Q$. Since $M^{\rho\tau} \leqslant M^\rho$, $M^{\rho\tau} = M^\rho$ as $\rho \in Q_d$. From $M_\rho = M_\sigma = M_\tau$, $M_\rho \leqslant M_{\rho\tau}$. This implies $M_\rho = M_{\rho\tau}$. Therefore $\rho\tau \in E(\sigma)$. Thus $E(\sigma)$ is a group of exponent p as each nontrivial element has minimal polynomial $(X - 1)^2$. Since $\rho\tau = \rho + \tau - 1$, $E(\sigma)$ is abelian. The rest of the proof is trivial.

In the rest of this section we assume that $p \geqslant 5$. First we need some ring results. Let K be an algebraic closure of $GF(p)$. For each x in K, each $f \in GF(p)[X]$ and each natural number n, let $a_n(x)$ be the n by n matrix

$$a_n(x) = \begin{pmatrix} x & I & & & \\ & x & I & & \\ & & \ddots & \ddots & \\ & & & x & I \\ & & & & x \end{pmatrix},$$

and $C_n(f)$ be the n by n matrix

$$C_n(f) = \begin{pmatrix} C(f) & I & & & \\ & C(f) & I & & \\ & & \ddots & \ddots & \\ & & & C(f) & I \\ & & & & C(f) \end{pmatrix},$$

where $C(f)$ is the companion matrix of f. For a partition μ whose parts are $n_1, \ldots, n_s$, let $a_\mu(x) = \operatorname{diag}(a_{n_1}(x), \ldots, a_{n_s}(x))$ and $C_\mu(f) = \operatorname{diag}(C_{n_1}(f), \ldots, C_{n_s}(f))$. Let $A(\mu, x)$ be the ring generated by $a_\mu(x)$, and let $F(\mu, x)$ be the set of p^a-th powers of elements of $A(\mu, x)$, where $p^a \geqslant \max\{n_1, \ldots, n_s\}$. We note that if $x \neq 0$, then $F(\mu, x)$ is a field isomorphic to $GF(p)(x)$ and $A(\mu, x) = F(\mu, x) \oplus R(\mu, x)$, where $R(\mu, x)$ is the radical of $A(\mu, x)$ and is the set of nilpotent elements of $A(\mu, x)$. Thus if $m = \max\{n_1, \ldots, n_s\}$, then $R(\mu, x)^m = 0$ but $R(\mu, x)^{m-1} \neq 0$. Also we note that if the polynomial f is monic and irreducible, then the ring generated by $C_\mu(f)$ is isomorphic to $A(\mu, x)$, where x is a root of f in K.

THEOREM 2.3 (Thompson). *Let $A = A(\mu, x)$, where μ is a non-empty*

partition and x is a nonzero element of K. Then $SL(2, A)$ is generated by $R(I)$ and $R'(a_\mu(x))$.

Proof. Let $R = R(\mu, x)$ and $F = F(\mu, x)$. Without loss of generality we may assume that $n = n_1 \geqslant \cdots \geqslant n_s$ are the parts of μ. For $1 \leqslant r \leqslant n$, let $P(r) = \{g \in SL(2, A) \mid g - I$ is a 2 by 2 matrix over $R^r\}$. Let $g = I + g_1 \in P(1)$ and $h = I + h_1 \in P(s)$ for some s between 1 and n, where g_1, h_1 are 2 by 2 matrices over R and R^s respectively. Since g_1h_1 and h_1g_1 are 2 by 2 matrices over R^{s+1}, $gh \equiv hg \pmod{R^{s+1}}$. Hence $[g, h] \in P(s + 1)$. Therefore $P(1) \geqslant \cdots \geqslant P(n) = 1$ is a central series of the p-group $P(1)$. For $1 \leqslant r \leqslant n - 1$ we have $R^r/R^{r+1} \cong F$ and $B(r) = P(r)/P(r + 1)$ is an elementary abelian p-group. Let $g \in P(r)$ and let $g_1 = g - I$. Then $g_1 = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, where $\alpha, \beta, \gamma, \delta \in R^r$. Since $g \in SL(2, A)$, $\alpha + \delta + \alpha\delta - \gamma\beta = 0$. Thus the mapping which associates g with g_1 induces an isomorphism between $B(r)$ and the additive group of 2 by 2 matrices over F with trace zero.

The exact sequence $0 \to R \to A \to F \to 0$ induces an exact sequence $1 \to P(1) \to SL(2, A) \to SL(2, F) \to 1$. Since $F \leqslant A$, the last sequence splits. With this observation we get the following.

(2.1). For $1 \leqslant r \leqslant n - 1$, $B(r)$ is isomorphic as a $SL(2, F)$-module to the additive group of 2 by 2 matrices over F with trace zero, where the action of $SL(2, F)$ is induced by conjugation. Furthermore this is an irreducible $SL(2, F)$-module.

We now apply induction on n to prove the Theorem. If $n = 1$, the result is a consequence of Dickson's theorem [5, Theorem 8.4, p. 44]. Let H be the group generated by the two displayed matrices. Suppose $n = n_1 = \cdots = n_r > n_{r+1} \geqslant \cdots \geqslant n_s$. Let ν be the partition whose parts are $n_1 - 1, \ldots, n_r - 1, n_{r+1}, \ldots, n_s$. Let $B = A(\nu, x)$. By induction we have $SL(2, B) = \langle R(I), R'(a_\nu(x))\rangle$. The mapping $\varphi(a_\mu(x)) = a_\nu(x)$ induces an exact sequence $0 \to R^{n-1} \to A \to B \to 0$. Let $H_0 = H \cap P(n - 1)$. Then $1 \to H_0 \to H \to SL(2, B) \to 1$ is an exact sequence. Hence $SL(2, A) = HP(n - 1)$. By (2.1) we see that $H \geqslant P(n - 1)$ if $H_0 \neq 1$. Hence we may assume that $H_0 = 1$. Suppose $n \geqslant 3$. Then $H \cap P(n - 2)$ covers $B(n - 2)$ and $H \cap P(1)$ covers $B(1)$. Now commutation in $P(1)$ induces a nonsingular pairing of $B(n - 2) \times B(1)$ into $P(n - 1)$. However, this contradictis $H_0 = 1$. Hence $n = 2$ and $H \cong SL(2, B) \cong SL(2, F)$. The map θ from H to $SL(2, F)$ which sends $R(I)$ to $R(I)$ and $R'(a_\mu(x))$ to $R'(a_\nu(x))$ extends to an isomorphism of H onto $SL(2, F)$. Since $H \cong SL(2, F)$ and the unique involution of $SL(2, A)$ is $i = \left(\begin{smallmatrix} -I & 0 \\ 0 & -I \end{smallmatrix}\right)$, $i \in H$. For each $t \in F$, let $\sigma(t) = \theta^{-1}(R(t))$ and $\tau(t) = \theta^{-1}(R'(t))$. Since $\sigma(t)$ centralizes $\sigma(1)$,

$$\sigma(t) = \begin{pmatrix} r & \sigma_0(t) \\ 0 & r \end{pmatrix}.$$

Since $\sigma(t)^p = 1$, $r^p = 1$. Since $\sigma(t) \in SL(2, A)$, $r^2 = 1$. Since $p \geqslant 5$, $r = 1$. Similarly we get $\tau(t) = R'(\tau_0(t))$. As

$$\left\{\begin{pmatrix} I & -I \\ 0 & I \end{pmatrix}\begin{pmatrix} I & 0 \\ I & I \end{pmatrix}\right\}^3 = \begin{pmatrix} -I & 0 \\ 0 & -I \end{pmatrix}$$

in $SL(2, F)$ we have $\{\sigma(-1)\,\tau(1)\}^3 = i$. This implies that $\tau_0(1) = I$. Let $A_0 = \{\sigma_0(t) \mid t \in F\}$. Since H contains $\sigma(1)\,\tau(-1)\,\sigma(1) = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$, $A_0 = \{\tau_0(t) \mid t \in F\}$. Thus A_0 is an additive subgroup of A containing I and $a_\mu(x)$. For $t \in F^\# = F\backslash\{0\}$, let

$$h(t) = \theta^{-1}\begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix}.$$

Then $h(t)$ normalizes $\{\sigma(s) \mid s \in F\}$ and $\{\tau(s) \mid s \in F\}$. Thus $h(t) = \mathrm{diag}(h_1(t), h_2(t))$ and $h_1(t)\,h_2(t) = 1$ as $h(t) \in SL(2, A)$. Since $h^{-1}(t)\,\sigma(t)\,h(t) \in \{\sigma(s) \mid s \in F\}$, $h_2(t)^2 \in A_0$. Let $q = |F|$. Then $q = |A_0|$. As $t^{q-1} = 1$ in F, $h_2(t)$ is a $(q-1)$ st root of unity in A. Hence $\{h_2(t) \mid t \in F\} \cong F^\#$. Thus $A_0 \geqslant (F^\#)^2 \cup \{a_\mu(x)\}$. Clearly $F^\#$ generates F additively. Since A_0 is an additive group, $A_0 \supset F \cup \{a_\mu(x)\}$. This implies that $|A_0| > q$, a contradiction. This completes the proof of the theorem.

Suppose $\sigma, \tau \in Q$ and $H = \langle \sigma, \tau \rangle$ is not a p-group. Let $\sigma - 1 = \alpha$, $\tau - 1 = \beta$ and $\Delta = \Delta(\sigma, \beta) = \alpha\beta + \beta\alpha$. Let $M = M_0 \oplus M_1 \oplus \cdots \oplus M_t$, where Δ is nilpotent on M_0, invertible on M_i for $i = i, \ldots, t$, and where the minimal polynomial of Δ on M_i is $(f_i)^{n_i}$, $f_0, \ldots, f_t$ being distinct monic irreducible polynomails in $GF(p)[x]$ and $f_0 = x$. Let $e_0, \ldots, e_t$ be the idempotents in $\mathrm{End}(M)$ such that $e_0 + \cdots + e_t = 1$, $e_i e_j = 0 = e_j e_i$ for $i \neq j$ and $M_i = Me_i$. Since H is not a p-group, Lemma 2.1 implies that $t \geqslant 1$. Let $H_i = He_i$. Since H commutes with Δ, H_i may be identified with a group of automorphisms of M_i. Let K_i be the largest subgroup of H which induces 1 on M_i. Then $H_i \cong H/K_i$.

Suppose $i \geqslant 1$. Since Δ annihilates $(M_i)_\sigma \cap (M_i)_\tau$ and Δ is invertible on M_i, $(M_i)_\sigma \cap (M_i)_\tau = 0$. Since $\alpha^2 = 0$, $(M_i)\alpha \leqslant (M_i)_\sigma$. From the exact sequence $0 \to (M_i)_\sigma \to M_i \to (M_i)\alpha \to 0$ we get that $|M_i/(M_i)_\sigma| = |(M_i)\alpha| = |(M_i)_\sigma|$. Thus $|M_i| \leqslant |(M_i)_\sigma|^2$. By symmetry we get $|M_i| \leqslant |(M_i)_\tau|^2$. Hence $|M_i| \leqslant |(M_i)_\sigma| \times |(M_i)_\tau| = |(M_i)_\sigma \oplus (M_i)_\tau|$. Therefore $M_i = (M_i)_\sigma \oplus (M_i)_\tau$, $(M_i)_\sigma = (M_i)_\alpha$ and $(M_i)_\tau = (M_i)\beta$. Let B_i be a basis for $M_i\beta$. Then $B_i\alpha$ is a basis for $M_i\alpha$ and $B_i \cup B_i\alpha$ is a basis for M_i. With respect to this basis, σ is represented by $R(I)$ and β is represented by $R'(u_i)$ for some square matrix u_i. Hence Δ is represented by $\mathrm{diag}(u_i, u_i)$. This implies that $u_i = c^{-1}C_{\mu_i}(f_i)c$ for some invertible matrix c and a non empty partition μ_i. Replacing B_i by another basis if necessary, we may assume that $u_i = C_{\mu_i}(f_i)$. Thus H_i may be identified with the subgroup of $SL(2, A(\mu_i, x))$ generated by $R(I)$ and $R'(a_{\mu_i}(\alpha_i))$, where α_i is a root of f_i in an algebraic closure K of $GF(p)$. By Theorem 2.3 we get

(2.2) $H_i \cong SL(2, A(\mu_i, \alpha_i))$, $i = 1,..., t$. These isomorphisms are given by $\alpha e_i = R(I)$ and $\tau e_i = R'(a_{\mu_i}(\alpha_i))$, $i = 1,..., t$.

Thus we get the following homomorphisms and exact sequences: $1 \to L_i \to H \xrightarrow{\varphi_i} SL(2, GF(p)(\alpha_i)) \to 1$, $i = 1,..., t$ where $\varphi_i(\sigma) = R(I)$ and $\varphi_i(\tau) = R'(\alpha_i)$. Next we argue that

(2.3) $H = L_iL_j$, $1 \leqslant i, j \leqslant t$, $i \neq j$.

Proof. Since $L_iL_j \trianglelefteq H$ and $L_iL_j/L_i \trianglelefteq H/L_i \cong SL(2, GF(p)(\alpha_i))$, we get that either (2.3) holds or $|L_iL_j/L_i| = 2$. Suppose (2.3) is false for i, j. Let $L_i^* \geqslant L_i$ such that $L_i^*/L_i = Z(H/L_i)$ and $L_j^* \geqslant L_j$ such that $L_j^*/L_j = Z(H/L_j)$. Then $L_i^* = L_j^*$. Hence $PSL(2, GF(p)(\alpha_i)) \cong H/L_i^* = H/L_j^* \cong PSL(2, GF(p)(\alpha_j))$ However this implies that the homomorphisms φ_i, φ_j induces an isomorphism from $SL(2, GF(p)(\alpha_i))$ to $SL(2, GF(p)(\alpha_j))$ which carries $R(I)$ to $R(I)$ and $R'(\alpha_i)$ to $R'(\alpha_j)$. This implies that $GF(p)(\alpha_i) = GF(p)(\alpha_j)$ and that isomorphism induces an automorphism of $GF(p)(\alpha_i)$ which carries α_i to α_j. Hence $f_i = f_j$. However this contradicts $i \neq j$. The proof of (2.3) is complete.

Define $b(\sigma, \tau) = \dim M_0$. Let $b = \max b(\sigma, \tau)$ where (σ, τ) ranges over all ordered pairs of elements of Q_d such that $\langle \sigma, \tau \rangle$ is not a p-group.

LEMMA 2.4. *If $\sigma, \tau \in Q_d$, $H = \langle \sigma, \tau \rangle$ is not a p-group and $b(\sigma, \tau) = b$, then $t = 1$, $n_1 = 1$ and H induces the identity transformation on M_0.*

Proof. Suppose $t \geqslant 2$. Let $N_i = \langle \sigma, L_i \rangle$ for $i = 1,..., t$. Thus N_i induces a p-group of automorphisms of M_i. If λ is a conjugate of σ in N_i, then $\langle \sigma, \lambda \rangle$ induces a p-group of automorphisms of $M_0 \oplus M_i$. By the definition of b, we get that $\langle \sigma, \lambda \rangle$ is a p-group. Thus $\sigma \in O_p(N_i)$ for $i = 1,..., t$ by Baer's theorem [5, Theorem 8.2, p. 105]. From (2.3) we see that $H = L_1L_2$. For any $S \leqslant H$, let $\bar{S} = SL_1/L_1$. Then $\{\bar{\sigma}^{\bar{H}}\} = \{\bar{\sigma}^{\bar{L}_2}\}$. Hence $\bar{\sigma} \in O_p(\bar{H})$ by Baer's theorem. However $O_p(\bar{H}) = 1$. Thus $\sigma \in L_1$. Since $\sigma \in O_p(N_1)$, $\sigma \in O_p(L_1) \leqslant O_p(H)$. This implies that H is a p-group which is impossible. Therefore $t = 1$.

Since H induces a p-group of automorphisms of M_0, K_1 is a p-group, where K_1 is the largest subroup of H which is 1 on M_1. Since $H/K_1 \cong H_1$ is perfect, $H = K_1T$, where T is the terminal member of the derived series of H. Thus $\sigma = su$, where $s \in K_1$ and $u \in T$. Since H induces a p-group on M_0, T is 1 on M_0. If $u = 1$, then $\sigma \in K_1$ and H is a p-group. This is impossible. Hence $u \neq 1$. Since s is 1 on M_1, σ agrees with u on M_1. Therefore $u \in Q$. Now $M^\sigma = M_0{}^\sigma \oplus M_1{}^\sigma$ and $M^u = M_0{}^u \oplus M_1{}^u = M_1{}^u = M_1{}^\sigma$. Since $\sigma \in Q_d$, $M_0{}^\sigma = 0$. By symmetry we get $M_0{}^\tau = 0$. This implies that H is 1 on M_0. Therefore $K_1 = 1$ and $H \cong H_1 \cong SL(2, A(\mu_1, \alpha_1))$. If $n_1 > 1$, then the radical R_1 of $A(\mu_1, \alpha_1) \neq 0$. Let $\rho \in R_1$ such that $\rho \neq 0$. Then H has an element η which maps to $R(\rho)$ in $SL(2, A(\mu_1, \alpha_1))$. This implies that $\eta \in Q$ and $M^\eta = M_1{}^\eta$ as H is 1 on M_0. Since ρ is nilpotent, $\dim M_1{}^\eta < \frac{1}{2} \dim M_1 = \dim M^\sigma$. This con-

tradicts $\sigma \in Q_d$. Therefore $R_1 = 0$ and $n_1 = 1$. The proof of the lemma is complete.

LEMMA 2.5. *If $\sigma, \tau \in Q_d$ and $H = \langle \sigma, \tau \rangle$ is not a p-group, then $t = 1$, $n_1 = 1$ and H is 1 on M_0. In particular $H \cong SL(2, p^a)$ for some natural number a.*

Proof. By Lemma 2.4 it suffices to show $b(\sigma, \tau) = b$. Since $| M/M_\sigma | = | M/M_\tau | = p^d$, $| M/M_\sigma \cap M_\tau | \leqslant p^{2d}$. Therefore $b \geqslant b(\sigma, \tau) \geqslant m - 2d$, where $m = \dim M$. Let $\sigma_0, \tau_0 \in Q_d$ such that $\langle \sigma_0, \tau_0 \rangle$ is not a p-group and $b = b(\sigma_0, \tau_0)$. Applying Lemma 2.4 to the pair (σ_0, τ_0) we see that the corresponding M_1 has dimension $2d$. Hence $b(\sigma_0, \tau_0) \leqslant m - 2d$. Therefore $b = m - 2d = b(\sigma, \tau)$ as required.

THEOREM 2.6. *Suppose $E, F \in \Sigma$ and $S = \langle E, F \rangle$ is not a p-group. Then*

(a) *$M = M^S \oplus M_S$ and $M^S = M^E \oplus M^F$.*

(b) *There is a basis for M^S such that with respect to this basis an element σ of E is represented by $R(a(\sigma))$ and an element τ of F is represented by $R'(b(\tau))$, where $W = \{a(\sigma) \mid \sigma \in E\}$ is a field of d by d matrices such that every nonzero element of K is an invertible matrix. Furthermore $\{b(\tau) \mid \tau \in F\} = W$ and $I \in W$.*

$$\text{(c)} \quad S \cong SL(2, W), \ | W | = | E | = | F |.$$

Proof. Since S is not a p-group, $E \not\leqslant O_p(S)$. Let $\sigma \in E \backslash O_p(S)$. By Baer's theorem there exists a conjugate τ of σ in S such that $H = \langle \sigma, \tau \rangle$ is not a p-group. Lemma 2.5 implies that $M^\sigma \cap M^\tau = 0$. Suppose $M^E \cap M^F = N \neq 0$. For any $s \in S$ we have $(1 - \sigma)s = s(1 - \sigma^s)$. Hence $(M^\sigma)s = M^{\sigma^s}$. Since $N \leqslant M_S$, $N = Ns \leqslant (M^\sigma)s \leqslant M^{\sigma^s}$. Therefore $N \leqslant M^\sigma \cap M^{\sigma^s}$.

Taking $\sigma^s = \tau$ we get a contradiction. Therefore $M^E \cap M^F = 0$. Hence $\langle x, y \rangle$ is not a p-group for any nontrivial elements $x \in E$ and $y \in F$ by Lemma 2.5. Let $1 \neq e \in E$, $1 \neq f \in F$ and $L = \langle e, f \rangle$. Thus $M = M^L \oplus M_L$ by Lemma 2.5. Hence $M^L \leqslant M^S$ and $M_L = M_e \cap M_f = M_E \cap M_F \leqslant M_S$. Therefore $M_L = M_S$, $M^L = M^S$ and $M = M^S \oplus M_S$. Now $M^S = M^L = M^e \oplus M^f = M^E \oplus M^F$. This gives (a). Since $(M^L)_L = 0$ and $L \cong SL(2, p^a)$ for some natural number a, Lemma 4.1 [2] implies that M^L has a basis and there exists a field J of d by d matrices such that L form the group of all matrices of the form $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ for $A, B, C, D \in J$, where $AD - BC = I$. Furthermore e is represented by $R(I)$. Thus $P_1 = \{R(B) \mid B \in J\}$ is a Sylow p-subgroup of L. Hence by considering conjugation by P_1, we may assume that f lies in $P_2 = \{R'(B) \mid B \in J\}$. By the definition of F an element τ in F is represented on M^S by $R'(b(\tau))$, where $b(\tau)$ is a nonsingular d by d matrice. Since $M = M^S \oplus M_S$, we may identify an element of S with its restriction on M^S. Thus we may identify an element

of S with its representing matrix on M^S. Since $\Delta(e, \tau)$ is invertible on M^S, $b(\tau)$ is invertible if $\tau \neq 1$. Let $W = \{b(\tau) \mid \tau \in F\}$. Then W is an additive group. Apply the argument of $\langle e, f \rangle$ to $\langle e, \tau \rangle$ we see that $b(\tau)^{-1} \in W$ if $b(\tau) \neq 0$. Since $R'(I) \in F$, $I \in W$. Lemma 4.3 of [2] implies that W is a field. By the definition of $E(\sigma)$, an element σ in E is represented by $R'(a(\sigma))$, where $a(\sigma)$ is a d by d matrice. Since S contains $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right) = R(I)\, R'(-I)\, R(I)$, $\{a(\sigma) \mid \sigma \in E\} = W$. This gives (b) and (c), and the proof of the theorem is complete.

For $E \in \Sigma$, let $I(E) = \{i \mid$ for some F in Σ, i is the involution of $\langle E, F \rangle\}$. For $1 \neq \sigma \in E$, let $U(E) = U(\sigma)$.

LEMMA 2.7. *If $i \in I(E)$, then i inverts M^E, centralizes M_E/M^E, and inverts M/M_E. In particular $ij \in U(E)$ for $i, j \in I(E)$.*

Proof. Let $F \in \Sigma$ such that $i \in \langle E, F \rangle$. Theorem 2.6 implies that $M = M^i \oplus M_i$, $M_i = M_E \cap M_F$, and $M^i = M^E \oplus M^F$. Since $M_E = M^E \oplus (M_E \cap M_F)$, the first conclusion follows. Let $i, j \in I(E)$. Then ij centralizes M^E, M_E/M^E, M/M_E which implies $ij \in U(E)$ as required.

THEOREM 2.8. *Suppose $E, F, F_1 \in \Sigma$. If $\langle E, F \rangle$ and $\langle E, F_1 \rangle$ share a common involution i, then $\langle E, F \rangle = \langle E, F_1 \rangle$.*

Proof. Let $S = \langle E, F \rangle$ and $S_1 = \langle E, F_1 \rangle$. By Theorem 2.6 we have $M = M^i \oplus M_i$, $M^i = M^S = M^{S_1}$ and $M_i = M_S = M_{S_1}$. Let $H = \langle E, F, F_1 \rangle$. We may identify H with a group of automorphisms of M^i. Theorem 2.6 implies that M^i has a basis and there exists a field of d by d matrices W such that an element σ of E is represented by $R(a(\sigma))$ and an element τ of F is represented by $R'(b(\tau))$, where $a(\sigma), b(\tau) \in W$. We identify an element of H with its representing matrix.

Case 1. $\langle F, F_1 \rangle$ is a p-group.

Let $N = M^i$. Suppose $[F, F_1] \neq 1$. By Theorem 1 of [2] we see that $N = N_F + N_{F_1}$ and $N^F \cap N^{F_1} = 0$. Since $0 \to N_F \to N \to N^F \to 0$ is exact, $\dim N = \dim N_F + \dim N^F$. Since $N^F \leqslant N_F$ and $\dim N = 2 \dim N^F$, we have $N^F = N_F$. Similary we get $N^{F_1} = N_{F_1}$. Since $\langle F, F_1 \rangle$ is a p-group, $N^F \cap N^{F_1} = N_F \cap N_{F_1} = N_{\langle F, F_1 \rangle} \neq 0$. This is impossible. Hence $[F, F_1] = 1$. Let $1 \neq s \in F_1$. Then $s = \left(\begin{smallmatrix} u & 0 \\ v & u \end{smallmatrix}\right)$, where u centralizes $W = \{b(\tau) \mid \tau \in F\}$. For each nonzero element t in W, let $h(t) = \left(\begin{smallmatrix} t^{-1} & 0 \\ 0 & t \end{smallmatrix}\right)$. Thus $h(t) \in S$ and $h(t)\, sh(t)^{-1} = \left(\begin{smallmatrix} u & 0 \\ tvt & u \end{smallmatrix}\right)$. If we choose t in the prime field, t is a scalar matrix. For such t, we get

$$\theta = s^{-1}h(t)\, sh(t)^{-1} = \begin{pmatrix} I & 0 \\ u^{-1}v(t^2 - I) & I \end{pmatrix}.$$

Thus $\theta \in F$. Since $p \geqslant 5$, there is an element k in $W \backslash \{0\}$ such that $k^2 \neq I$. Taking $t = k$, we conclude that $b = u^{-1}v \in W$. Let $w = u - I$. Since $s \in Q$,

$(s-I)^2=0$. This implies that $w^2=0$, and $ubw+wub=0$. As $u=I+w$, we get $0=bw+wbw+wb$. Right multiplication by w gives $wbw=0$. Thus $0=bw+wb$. Since u centralizes W, w commutes with b. Hence $0=2bw$. Since $p\neq 2$, $0=bw$. If $b=0$, then $v=ub=0$. This implies that s centralizes E which is impossible as $\langle E, F_1\rangle \cong SL(2, W)$. Therefore $b\neq 0$ and b is invertible. Thus $w=0$ and $u=I$. Therefore $s\in F$ and $F=F_1$ in this case.

Case 2. $\langle F, F_1\rangle$ is not a p-group.

By case 1, we may assume that $\langle F_1, F\rangle$ is not a p-group for any Sylow p-subgroup T of S. Let $1\neq \varphi\in F_1$ and let

$$\varphi=\begin{pmatrix} I+\alpha & \beta \\ \gamma & I+\delta \end{pmatrix},$$

where α, β, γ, δ are d by d matrices. Applying Theorem 2.6 to $\langle E, F_1\rangle$ we see that there exists an element $R(t)$ in E such that $\Delta(\varphi, R(t))=I$, where $t\in W$. This implies that $t\neq 0$, $\gamma=t^{-1}\in W$ and $\alpha t+t\alpha=0$. Applying Theorem 2.6 to $\langle F, F_1\rangle$ we get an element $R'(u)$ in F such that $\Delta(\varphi, R'(u))=I$. This gives $u\neq 0$, $\beta=u^{-1}\in W$ and $\delta u+u\delta=0$. Let $e=R(v)\in E$. Then

$$e^{-1}\varphi e=\begin{pmatrix} I+\alpha-v\gamma & \beta+\alpha v-v\delta-v\gamma v \\ \gamma & I+\gamma v+\delta \end{pmatrix}.$$

Now $\langle F_1{}^e, E\rangle \cong SL(2, W)\cong \langle F_1{}^e, F\rangle$. Applying the above argument to $e^{-1}\varphi e$ we conclude that $\beta+\alpha v-v\delta-v\gamma v\in W$ for all $v\in W$. Since β and γ belong to W, $\alpha v-v\delta\in W$ for all $v\in W$. Since $\delta=-\gamma\alpha\gamma^{-1}$, $\alpha v+v\gamma\alpha\gamma^{-1}\in W$ for all $v\in W$. Let $\phi=v\gamma$. Then for $\phi\in W$ we have $\alpha\phi+\phi\alpha\in W$. Taking $\phi=1$, we get $\alpha\in W$ as $p\neq 2$. Since $\delta=-\gamma\alpha\gamma^{-1}$ and $\gamma\in W$, $\delta\in W$. Since $\varphi\in Q$, $\alpha^2+\beta\gamma=0$ and $\alpha\beta+\beta\delta=0$. Since α, β, γ, $\delta\in W$ and $\beta\neq 0$, we have $\delta=-\alpha$. This shows that $\varphi\in S$. Let P be a Sylow p-subgroup of S containing φ. Then $P\in\Sigma$. Lemma 2.2 implies that $F_1=P$. Therefore $S=S_1$ and the proof of the theorem is complete.

LEMMA 2.9. *Let $\sigma\in Q$ and R a p'-group of G. If σ normalizes R, then σ centralizes R. In particular $O_{p'}(G)\leqslant Z(G)$.*

Proof. Let $H=\langle\sigma, R\rangle$. Suppose $O_p(H)=1$. Since $p\geqslant 5$, Theorem B of [8] implies that $M(\sigma-1)^2\neq 0$. This contradicts $\sigma\in Q$. Therefore $O_p(H)\neq 1$. Since $|H|=p|R|$ and $|R|$ is prime to p, $\sigma\in O_p(H)$. The rest of the proof is now clear.

We now give the definition and some basic properties of the "generalized Fitting subgroup." A group is quasi-simple if it is perfect and the quotient over its center is simple. For any group H, let $E(H)$ be the central product of all subnormal quasi-simple subgroups of H. These subnormal subgroups are called

the components of $E(H)$. We define $F^*(H) = E(H)F(H)$, where $F(H)$ is the Fitting subgroup of H.

LEMMA 2.10. (a) *If L is a component of $E(H)$ and $X \leqslant H$, then $L \leqslant [L, X]$ or $[L, X] = 1$. If X is L-invariant, then $L \leqslant E(X)$ or $[L, X] = 1$. Moreover, $[E(H), X]$ is the product of those components of $E(H)$ not centralized by X.*

$$\text{(b)} \quad C_H(F^*(H)) \leqslant F^*(H).$$

Proof. See (2.1) and (2.2) of [4].

THEOREM 2.11. *If $O_p(G) = 1$ and $G = \langle \sigma \mid \sigma \in Q \rangle$, then $G = E(G)$. Let $S_1, \ldots, S_n$ be the components of $E(G)$. Then $Q_d = \bigcup_{i=1}^n (Q_d \cap S_i)$ and $S_i = \langle \sigma \mid \sigma \in Q(S_i, M) \rangle$.*

Proof. For each nonnegative integer f, let $Q_f = \{\sigma \in Q \mid d(\sigma) = f\}$. We will prove by induction on f that $Q_f \leqslant E(G)$. If $f < d$, then $Q_f = \varnothing$. Since $O_p(G) = 1$, Lemmas 2.9 and 2.10 imply that $C_G(E(G)) \leqslant Z(G)$. Let $\sigma \in Q_d$. Since $\sigma \notin O_p(E(G)\langle\sigma\rangle)$, there exists $x \in E(G)$ such that $\langle \sigma, \sigma^x \rangle$ is not a p-group. Lemma 2.5 implies that $\sigma \in \langle \sigma, \sigma^x \rangle = \langle \sigma, \sigma^x \rangle' \leqslant E(G)$. Therefore $Q_d \leqslant E(G)$.

Suppose now $f > d$, and that if $f > f_0$, then $Q_{f_0} \leqslant E(G)$. Suppose $\sigma \in Q_f$ and $\sigma \notin E(G)$. Since $\sigma \notin O_p(E(G)\langle\sigma\rangle)$, there exists $x \in E(G)$ such that $H = \langle \sigma, \sigma^x \rangle$ is not a p-group. By (2.2) we see that the terminal member T of H is not trivial. We may therefore assume $H = T\langle\sigma\rangle$. Since $T \leqslant H' \leqslant E(G)$, $\sigma \notin T$. Let $\Delta = \Delta(\sigma, \sigma^x)$ and let $M = M_0 \oplus \cdots \oplus M_t$ be the Δ-decomposition of M. Since T is perfect, T induces 1 on M_0. Also T and H induce the same group of automorphisms on $N = M_1 \oplus \cdots \oplus M_t$. Hence there exists $\rho \in T$ such that $\sigma\rho^{-1}$ is 1 on N and $\sigma\rho^{-1}$ agrees with σ on M_0. Hence $\sigma\rho^{-1} \in Q$ or $\sigma\rho^{-1} = 1$. Since $\sigma \notin T$, $\sigma\rho^{-1} \in Q$. However $M^{\sigma\rho^{-1}} = (M_0)^\sigma \nleqslant M^\sigma$ as σ does not induce 1 on N. This implies that $\sigma\rho^{-1} \in Q_{f_0}$ with $f_0 < f$. Hence $\sigma\rho^{-1} \in E(G)$ by induction and so $\sigma = (\sigma\rho^{-1})\rho \in E(G)$. This contradiction shows that $Q_f \leqslant E(G)$. Therefore $G = E(G)$.

Let $S_1, \ldots, S_n$ be the components of $E(G)$. Let $\sigma \in Q_d$. Then $\sigma = \sigma_1 \cdots \sigma_n$, where $\sigma_i \in S_i$ for $i = 1, \ldots, n$. Since $\sigma \neq 1$, there exists j such that $\sigma_j \neq 1$. Since $[\sigma_i, S_j] = 1$ for $i \neq j$ and $Z(S_j)$ is a p'-group, $[\sigma, S_j] = [\sigma_j, S_j] \neq 1$. Hence $\sigma \notin O_p(S_j\langle\sigma\rangle)$ and there exists $x \in S_j$ such that $\langle \sigma, \sigma^x \rangle$ is not a p-group. Lemma 2.5 now implies $\sigma \in S_j$. Thus $Q_d = \bigcup_{i=1}^n (Q_d \cap S_i)$.

For $\gamma \in Q$, we have $\gamma = \gamma_1 \cdots \gamma_n$, where $\gamma_i \in S_i$, $\gamma_i{}^p = 1$ and γ_i is uniquely determined by γ. We now claim the following.

(2.4) $\gamma_i = 1$ or γ_i is a product of elements of $Q \cap S_i$.

We will prove (2.4) by induction on f that the elements of Q_f satisfy (2.4). If $f < d$, then $Q_f = \varnothing$. Since $Q_d = \bigcup_{i=1}^n (Q_d \cap S_i)$, (2.4) holds for elements in

Q_d. Suppose now $d < f$, and that if $f_0 < f$, then (2.4) holds for elements in Q_{f_0}. Let $\sigma \in Q_f$ and σ does not satisfy (2.4). Let $\sigma = \sigma_1 \cdots \sigma_n$, where $\sigma_i \in S_i$, $i = 1,\ldots, n$. Let $J = \{i \mid \sigma_i \neq 1\}$. If $|J| = 1$, then (2.4) is satisfied by σ. Thus $|J| \geqslant 2$. Without loss of generality we may assume $\{1, 2\} \leqslant J$. Let $s = \sigma_1$ and $t = \sigma\sigma_1^{-1}$. Then $[S_1, t] = 1$. Since $s^p = 1$ and $O_p(S_1) = 1$, there exist $u \in S_1$ such that $\langle s, s^u \rangle$ is not a p-group. Let $\tau = \sigma^u$. Thus $H = \langle \sigma, \tau \rangle$ is not a p-group. Since $\sigma^u = s^u t$, $H' \leqslant S_1$. Since $\sigma \notin S_1$, H is not perfect. Let $\Delta = \Delta(\sigma, \tau)$ and let $M = M_0 \oplus M_1 \oplus \cdots \oplus M_t$ be the Δ-decomposition of M. Set $N = M_1 \oplus \cdots \oplus M_t$. Since H is not a p-group. $N \neq 0$. Let D be the largest subgroup of H which is 1 on N. Then D is a p-group and H/D is perfect. Thus $H = DT$ where T is the terminal member of the derived series of H. Since T is perfect, T induces 1 on M_0. Since T and H induces the same group of automorphisms of N, $T = \langle \xi, \eta \rangle$ where ξ agrees with σ on N and η agrees with τ on N. Thus $\xi \in Q$. Since H is not perfect, $M_0 \neq 0$ and $H \neq T$. Since $M^\xi = N^\xi = N^\sigma < M^\sigma$, $\xi \in Q_e$ with $e < f$. Let $\delta = \sigma\xi^{-1}$. Then δ agrees with σ on M_0 and is 1 on N. Since $M_0 \neq 0$, $\delta \neq 1$. Therefore $\delta \in Q$. Since $M^\delta = M_0{}^\delta = M_0{}^\sigma < M^\sigma$, $\delta \in Q_g$ with $g < f$. By induction we have $\xi = \xi_1 \cdots \xi_n$, $\delta = \delta_1 \cdots \delta_n$, where ξ_i, δ_i are either 1 or the product of elements in $Q \cap S_i$. Since $\sigma = \xi\delta = (\xi_1\delta_1) \cdots (\xi_n\delta_n)$, σ also satisfies (2.4). This contradiction shows that (2.4) holds for all elements in Q.

Since S_i is quasi-simple and $O_p(S_i) = 1$, it suffices to show that $Q \cap S_i \neq \emptyset$, for $i = 1,\ldots, n$. If $\gamma_i = 1$ for all $\gamma \in Q$, then $S_i = 1$ as $G = \langle \gamma \mid \gamma \in Q \rangle$. This is impossible. Therefore there exists $\sigma \in Q$ such that $\sigma_i \neq 1$. By (2.4) we see that $Q \cap S_i \neq \emptyset$. This completes the proof of the theorem.

We remark that unlike the central product theorem of [13], in general $Q \neq \bigcup_{i=1}^n (Q \cap S_i)$. Although $Q_d = \bigcup_{i=1}^n (Q_d \cap S_i)$ but $Q_d(S_i, M)$ is not necessarily equal to $Q_d \cap S_i$. In fact an easy example shows that $Q_d \cap S_i$ might be the empty set.

3. p-Groups

The following lemma's short proof is provided by Professor Glauberman.

LEMMA 3.1. *Let P be a p-group, p a prime. Suppose E and F are two normal subgroups of P. If $P = EF$, then* $\mathrm{cl}(P) \leqslant \mathrm{cl}(E) + \mathrm{cl}(F)$.

Proof. Let $\mathrm{cl}(E) = a$ and $\mathrm{cl}(F) = b$. Theorem 10.3.2 of [7] implies that $P_{a+b+1} = \langle P_{a+b+2}, [x_1,\ldots, x_{a+b+1}] \mid x_i \in E \cup F$ for $i = 1,\ldots, a + b + 1 \rangle$. Each subset $\{x_1,\ldots, x_{a+b+1}\}$ in $E \cup F$ contains either $a + 1$ elements of E or $b + 1$ elements of F. Since E and F are normal subgroups of P, $[x_1,\ldots, x_{a+b+1}] = 1$. Therefore $P_{a+b+1} = P_{a+b+2}$. This implies $P_{a+b+1} = 1$ and $\mathrm{cl}(P) \leqslant \mathrm{cl}(E) + \mathrm{cl}(F)$ as required.

LEMMA 3.2. *Let p be a prime and M a vector space over the field K with p elements. Suppose P is a p-group acting faithfully on M. If $Q(P, M) = \{\sigma \in P \mid \sigma^p = 1, \sigma \neq 1\}$ and $P = \{1\} \cup Q(P, M)$, then* $\mathrm{cl}(P) \leqslant 2$.

Proof. If $p = 2$, then P is abelian as every element has order 1 or 2. Suppose $p \geqslant 3$. Let N be the K-module of $\mathrm{End}_K(M, M)$ generated by the elements $g - 1$ as g ranges over P. Let $e, f \in Q(P, M)$. Set $\alpha = e - 1$ and $\beta = f - 1$. Then $\alpha^2 = 0 = \beta^2$. Therefore $e^a = 1 + a\alpha$ and $f^b = 1 + b\beta$ for any integers a and b. Since $P = \{1\} \cup Q(P, M)$, $(e^a f^b - 1)^2 = 0$ for all integers a and b. Thus $0 = (e^a f^b - 1)^2 = \{(e^a - 1)(f^b - 1) + (e^a - 1) + (f^b - 1)\}^2 = a^2 b^2 (\alpha\beta)^2 + a^2 b \alpha\beta\alpha + ab\alpha\beta + ab^2 \beta\alpha\beta + ab\,\beta\alpha$. Since P has exponent p, we may restrict our values a and b in Z/pZ which we may identify with K. The above equation implies that for all $a, b \in K$, $0 = ab(\alpha\beta)^2 + a\alpha\beta\alpha + \alpha\beta + b\beta\alpha\beta + \beta\alpha$ if $ab \neq 0$. Let a_1, b_1, a_2, b_2 be nonzero elements in K. Substituting these values for a, b in the last equation, we get two equations. Substracting these last two equations we get

$$0 = (a_1 b_1 - a_2 b_2)(\alpha\beta)^2 + (a_1 - a_2)\,\alpha\beta\alpha + (b_1 - b_2)\,\beta\alpha\beta. \tag{3.1}$$

Since $p \geqslant 3$, we can choose two nonzero elements a_1, a_2 in K such that $a_1 \neq a_2$. Let $b_1 = b_2$ be any nonzero element in K. Then (3.1) implies that $0 = b_1(\alpha\beta)^2 + \alpha\beta\alpha$ for any $0 \neq b_1 \in K$. Since $|K| \geqslant 3$, we must have $(\alpha\beta)^2 = 0$. Therefore $\alpha\beta\alpha = 0$. Now (3.1) implies that $\beta\alpha\beta = 0$. From $(ef - 1)^2 = 0$ we now get

$$(e - 1)(f - 1) + (f - 1)(e - 1) = 0. \tag{3.2}$$

Since (3.2) is clearly true for $e = f = 1$, (3.2) is valid for all elements e, f in P.

Let $g, h, k \in P$ and let $\gamma = g - 1$, $\delta = h - 1$ and $\xi = k - 1$. Thus $gh - 1 = (g - 1)(h - 1) + (g - 1) + (h - 1) = \gamma\delta + \gamma + \delta$. Hence $(gh - 1)(k - 1) = \gamma\delta\xi + \gamma\xi + \delta\xi$. Applying (3.2) to $e = gh$ and $f = k$ we get $(gh - 1)(k - 1) = -(k - 1)(gh - 1) = -\xi\gamma\delta - \xi\gamma - \xi\delta$. Applying (3.2) to $e = g$ and $f = k$ we get $\gamma\xi = -\xi\gamma$. Similarly we have $\delta\xi = -\xi\delta$. Therefore $\gamma\delta\xi + \gamma\xi + \delta\xi = -\xi\gamma\delta - \xi\gamma - \xi\delta$ implies $\gamma\delta\xi + \xi\gamma\delta = 0$. Therefore $0 = \gamma\delta\xi + \xi\gamma\delta = 2\gamma\delta\xi$. Since $p \neq 2$, $\gamma\delta\xi = 0$. Since g, h and k are arbitrary, we get $N^3 = 0$. Since $x - 1 \in N^k$ for all $x \in P_k$, $P_3 = 1$. Therefore $\mathrm{cl}(P) \leqslant 2$ as required.

THEOREM 3.3. *Let P be a p-group acting faithfully on the vector space M over the field K with p elements, $p \geqslant 5$. Suppose $Q(P, M) = \{\sigma \in P \mid \sigma \neq 1, \sigma^p = 1\}$ and $P = \langle \sigma \mid \sigma \in Q(P, M) \rangle$. Then* $\mathrm{cl}(P) \leqslant 2$ *and* $\exp(P) \leqslant p$.

Proof. Without loss of generality we may assume $P \neq 1$. Let N be the K-module of $\mathrm{End}_K(M, M)$ generated by $g - 1$ as g ranges over P. Let $Q \leqslant Q(P, M)$ such that $P = \langle \sigma \mid \sigma \in Q \rangle$ but P is not generated by any proper subset of Q. If $|Q| \leqslant 1$, then the result is quite clear. Suppose $|Q| \geqslant 2$. Let $e, f \in Q$.

Set $F = \langle \sigma \mid \sigma \in Q,\ \sigma \neq e \rangle^P$ and $E = \langle \sigma \mid \sigma \in Q, \sigma \neq f \rangle^P$. Since $\langle \sigma \mid \sigma \in Q, \sigma \neq e \rangle \leqslant P$, $F \nleqslant P$. By induction we get that $\mathrm{cl}(F) \leqslant 2$ and $\exp(F) \leqslant p$. Similarly we have $\exp(E) \leqslant p$ and $\mathrm{cl}(E) \leqslant 2$. Clearly E and F are normal subgroups of P satisfying $P = EF$. Lemma 3.1 implies that $\mathrm{cl}(P) \leqslant 4$. Since $p \geqslant 5$, P is regular. Since $P = \langle \sigma \mid \sigma \in Q \rangle$, $P = F\langle e \rangle$. Let $x \in F$ and a an integer. Since P is regular and $\exp(F) \leqslant p$, (12.4.1) of [7] implies that $1 = x^p(e^a)^p = (xe^a)^p \prod_i (D_i)^p$ where $D_i \in P' \leqslant F$. Hence $(xe^a)^p = 1$. This shows that $\exp(P) = p$. Therefore $P = Q(P, M) \cup \{1\}$. Lemma 3.2 implies that $\mathrm{cl}(P) \leqslant 2$ as required.

LEMMA 3.4. *Let p be an odd prime and M a vector space over the field K with p elements. Let P be a p-group acting faithfully on M. Suppose $Q(P, M) = \{\sigma \mid \sigma \neq 1, \sigma^p = 1\}$. If $P = \langle e, f \rangle$ for some $e, f \in Q_d(P, M)$, then P is elementary abelian.*

Proof. Since $e^p = f^p = 1$, it suffices to show that P is abelian. Suppose P is not abelian. Let $g = [e, f]$. Theorem 1 of [3] shows that $g \in Q_d(P, M)$, $\mathrm{cl}(P) \leqslant 2$ and $P \leqslant U(g)$. Since $p \geqslant 3$, P is regular. Hence $(ef)^p = 1$. Since P is nonabelian, $ef \neq 1$. Therefore $ef \in Q(P, M)$. Since $g \in Q_d(P, M)$, M has a basis such that g is represented by

$$\begin{pmatrix} I_d & I_d & 0 \\ 0 & I_d & 0 \\ 0 & 0 & I \end{pmatrix}.$$

We identify an element of P with its representative matrix with respect to this basis. We label an element σ of $U(g)$ by (a, b, c) provided

$$\sigma = \begin{pmatrix} I & c & a \\ 0 & I & 0 \\ 0 & b & I \end{pmatrix}.$$

Let $e = (\alpha, \beta, \gamma)$ and $f = (\xi, \eta, \delta)$. Then $[e, f] = (0, 0, \alpha\eta - \xi\beta)$. Therefore $\alpha\eta - \xi\beta = I$. Since $e, f \in Q_d(P, M)$, we get $\alpha\beta = 0 = \xi\eta$. Since $ef \in Q(P, M)$, $(ef - 1)^2 = 0$ and so $0 = (\alpha + \xi)(\beta + \eta)$. Hence $0 = \alpha\eta + \xi\beta$. From $\alpha\eta - \xi\beta = I$ we now get $2\alpha\eta = I$. Therefore $\mathrm{rank}\ \alpha = d = \mathrm{rank}\ \eta$. Since $\xi\beta = -\alpha\eta$, $\mathrm{rank}\ \xi = d = \mathrm{rank}\ \beta$. However this implies that $d = \mathrm{rank}(e - 1) = \mathrm{rank} \begin{pmatrix} \gamma & \alpha \\ \beta & 0 \end{pmatrix} \geqslant d$, a contradiction. This completes the proof of the lemma.

COROLLARY 3.5. *Let p be an odd prime and M a vector space over the field K with p elements. Let G act faithfully on M such that $Q(G, M) = \{\sigma \mid \sigma \in G, \sigma^p = 1\}$. If $E, F \in \mathcal{E}(G, M)$ such that $\langle E, F \rangle$ is a p-group, then $\langle E, F \rangle$ is elementary abelian.*

Proof. This is a consequence of Lemma 4.2 of [3] and the previous lemma.

4. Theorems A and B

In this section we assume the hypothesis of Theorem A, namely, the following condition.

(4.1) M is a vector space over $GF(p)$, $p \geqslant 5$ and G is a group acting faithfully on M such that $Q(G, M) = \{\sigma \mid \sigma \neq 1, \sigma^p = 1\}$ and $G = \langle \sigma \mid \sigma \in Q(G, M) \rangle \neq 1$.

We set $Q = Q(G, M)$, $d = d(G, M)$, $Q_d = Q_d(G, M)$ and $\Sigma = \Sigma(G, M)$. We now convert Σ into an undirected graph as follows. The vertices are the elements of Σ. Two elements X and Y in Σ are connected if $\langle X, Y \rangle$ is not a p-group. A connected component containing X is denoted by $W(X)$. We write $Y \in W(X)$ to mean that Y is a vertex in $W(X)$.

Lemma 4.1. *Let $X, Y \in \Sigma$. If $W(X) \neq W(Y)$, then $[X, Z] = 1$ for all $Z \in W(Y)$.*

Proof. Let $Z \in W(Y)$. If $\langle X, Z \rangle$ is not a p-group, then $W(X) = W(Z) = W(Y)$ which is impossible. Therefore $\langle X, Z \rangle$ is a p-group. Corollary 3.5 implies that $[X, Z] = 1$ as required.

Theorem 4.2. *Let $E \in \Sigma$. If $E \not\leqslant O_p(G)$, then $\langle Y \mid Y \in W(E) \rangle \cong SL(2, \mid E \mid)$.*

Proof. Since $E \not\leqslant O_p(G)$, there exists $1 \neq e_1 \in E$ such that $e_1 \notin O_p(G)$. By Baer's theorem there is a conjugate f_1 of e_1 such that $\langle e_1, f_1 \rangle$ is not a p-group. Let $F = E(f)$. Then $F \in W(E)$. By Theorem 2.6, M has a basis such that an element σ of E is represented by

$$\begin{pmatrix} I & a(\sigma) & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix},$$

an element τ of F is represented by

$$\begin{pmatrix} I & 0 & 0 \\ b(\tau) & I & 0 \\ 0 & 0 & I \end{pmatrix},$$

and $W = \{a(\sigma) \mid \sigma \in E\} = \{b(\tau) \mid \tau \in F\}$ is a field of d by d matrices such that the nonzero elements of W are invertible. We identify an element of G by its representing matrix with respect to this basis. Let $e \in E$ such that $a(e) = I$ and $f \in F$ such that $b(f) = I$. Let $U = U(E) = U(e)$. We label an element u of U by (λ, μ, ν) provided

$$u = \begin{pmatrix} I & \nu & \lambda \\ 0 & I & 0 \\ 0 & \mu & I \end{pmatrix}.$$

Since $(\lambda, \mu, \nu)(\xi, \eta, \xi) = (\lambda + \xi, \mu + \eta, \nu + \zeta + \lambda\eta)$, $\exp(U) = p$. Let i be the involution of $\langle E, F\rangle$. Then (λ, μ, ν) is inverted by i if and only if $\nu = \frac{1}{2}\lambda\mu$. Let

$$\omega = \begin{pmatrix} 0 & I & 0 \\ -I & 0 & 0 \\ 0 & 0 & I \end{pmatrix}.$$

Then $\omega \in \langle E, F\rangle$. Let $1 \neq \theta = (\alpha, \beta, \gamma)$ be inverted by i. For $t \in W\backslash\{0\}$, let

$$h(t) = \begin{pmatrix} t^{-1} & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & I \end{pmatrix},$$

$X_{a+b}(t) = \theta^{h(t)}$, $X_b(t) = X_{a+b}(t)^\omega$ and $X_{2a+b}(t) = [X_{a+b}(t), X_b(\frac{1}{2})]$. Then

$$X_{2a+b}(t) = \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & I + \beta t\alpha \end{pmatrix}.$$

By (4.1) we have $\theta \in Q$. Hence $\theta = (\alpha, \beta, 0)$.

Case 1. $\beta\alpha = 0$.

We may view β as a linear transformation from a vector space V of dimension $m - 2d$ to a vector space T of dimension d over $GF(p)$ and α as a linear transformation from T to V. Since $\beta\alpha = 0$, $\operatorname{Im}\beta \leqslant \operatorname{Ker}\alpha$. Hence $\operatorname{rank}(\theta - I) = \operatorname{rank}\alpha + \operatorname{rank}\beta \leqslant \dim \operatorname{Im}\alpha + \dim \operatorname{Ker}\alpha = d$. Therefore $\theta \in Q_d$ by the definition of d. However this implies $X_b(1) \in Q_d$ and $[e, X_b(1)] = X_{a+b}(1) \in Q_d$. Hence $\langle e, X_b(1)\rangle$ is a nonabelian p-group. This contradicts Lemma 3.4. Therefore case (1) cannot occur.

Case 2. $\beta\alpha \neq 0$.

Since $\alpha\beta = 0$ and $\beta\alpha \neq 0$, $X_{a+2b}(1) \in Q$. Therefore $d \leqslant \operatorname{rank}(X_{2a+b}(1) - I) = \operatorname{rank}\beta\alpha$. Since α is a d by $m - 2d$ matrix and β is an $m - 2d$ by d matrix, we have $\operatorname{rank}\beta\alpha \leqslant d$. Hence $d = \operatorname{rank}\beta\alpha$ and $X_{2a+b}(1) \in Q_d$. Let $P = \langle E, X_b(t), X_{a+b}(t), X_{2a+b}(t) \mid t \in W\backslash\{0\}\rangle$. From $[e, X_b(1)] = X_{a+b}(1)$ $X_{2a+b}(1)$ and $[X_{2a+b}(1), X_b(\frac{1}{2})] = 1$ we get $[[e, X_b(1)]\, X_b(\frac{1}{2})] = [X_{a+b}(1), X_b(\frac{1}{2})] = X_{2a+b}(1)$. Hence $\operatorname{cl}(P) \geqslant 3$. This contradicts Theorem 3.3 as $P = \Omega_1(P)$. Therefore case 2, also, cannot occur.

Hence no nontrivial element of U is inverted by i. Lemma 2.7 implies that $I(E) = \{i\} = I(F)$. Since $W(E)$ is connected, Theorem 2.8 implies $\langle Y \mid Y \in W(E)\rangle \cong SL(2, \mid E \mid)$ as required.

THEOREM B. *If in addition to hypothesis* (4.1) *we also assume that* $\mid M(\sigma - 1)\mid =$

$|M(\tau - 1)|$ *for any* $\sigma, \tau \in Q$, *then either* G *is an elementary abelian* p*-group or* $G \cong SL(2, p^a)$ *for some positive integer* a.

Proof. Under our assumption we have $Q = Q_d$. If G is a p-group, then G is an elementary p-group by Lemma 3.4. Suppose $G \neq O_p(G)$. Let $e \in Q \backslash O_p(G)$. Then there is a conjugate f of e such that $\langle e, f\rangle$ is not a p-group. Lemma 2.5 implies that $H = \langle e, f\rangle \cong SL(2, p^n)$ for some positive integer n and M has a basis such that the representing matrices for e and f are

$$\begin{pmatrix} I & I & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix}, \qquad \begin{pmatrix} I & 0 & 0 \\ A & I & 0 \\ 0 & 0 & I \end{pmatrix},$$

respectively, where A is a non-singular d by d matrix. We identify an element of G by its representing matrix with respect to this basis. Let $x \in Q \cap C_G(H)$. Then $x = \mathrm{diag}(B, B, C)$, where B is a d by d matrix and C is a $m - 2d$ by $m - 2d$ matrix. Suppose $x \neq 1$. Since $x \in C_G(H)$, $x \notin \langle e\rangle$ and $x \notin \langle f\rangle$. Since $(xe)^p = 1$, $xe \in Q$. This implies that $2B(B - I) = 0$. Since $p \neq 2$ and B is invertible, $B = I$. Since $Q = Q_d$, $\mathrm{rank}(xe - I) = d$. This implies rank $(C - I) = 0$. Hence $C = I$ and $x = 1$, a contradiction. Therefore $Q \cap C_G(H) = \varnothing$. By Lemma 3.4 we now see that $O_p(G) = 1$. Theorem 2.11 implies $G = E(G)$. Since $Q \cap C_G(H) = \varnothing$, G has only one component. Hence G is quasi-simple. Theorem 4.2 now yields the proof of the theorem.

We now give the proof of Theorem A in the rest of this section. First we will prove $G = F^*(G)$ by showing that $Q_f \leqslant F^*(G)$ for $f = 1, \ldots$. We apply induction on f to show the last fact. If $f < d$, then $Q_f = \varnothing$. If $E \in \Sigma$ and $E \not\leqslant O_p(G)$, Theorem 4.2 implies that $E \leqslant E(G)$. This shows that $Q_d \leqslant F^*(G)$.

We may now suppose that $d < f$, and that if $f_0 < f$, then $Q_{f_0} \leqslant F^*(G)$. Suppose $\sigma \in Q_f$ and $\sigma \notin F^*(G)$. Thus $\sigma \notin O_p(G)$. By Baer's theorem there exists a conjugate γ of σ such that $\langle \sigma, \gamma\rangle$ is not a p-group. If $[\sigma, E(G)] \neq 1$, we may choose $\gamma \in E(G)\langle\sigma\rangle$ and we will do so. Let $H(\gamma) = \langle \sigma, \gamma\rangle$. Among all possible subgroups $H(\gamma)$ we choose $H = H(\tau)$ with minimal order. Let $\Delta = \Delta(\sigma, \tau)$ and let $M = M_0 \oplus M_1 \oplus \cdots \oplus M_t$ be the Δ-decomposition of M as in Section 2. The notation in Section 2 is now used here. By (2.2) we see that the terminal member of the derived series of H is nontrivial and T induces the same group of automorphisms on $N = M_1 \oplus \cdots \oplus M_t$ as H induces. Without loss of generality we may assume that $H = T\langle\sigma\rangle$. Since T is perfect, T induces 1 on M_0. Suppose $[\sigma, E(G)] \neq 1$. Then $T \leqslant E(G)$. There is $\rho \in T$ such that $\sigma\rho^{-1}$ induces 1 on N. Since $\sigma \notin E(G)$, H does not induce 1 on M_0. Since T is 1 on M_0, $H = \langle\sigma\rho^{-1}\rangle \times T$ Thus $\sigma\rho^{-1} \in Q_{f_0}$ for some $f_0 \leqslant f$. If $f_0 < f$, then $\sigma\rho^{-1} \in F^*(G)$ by induction and $\sigma = (\sigma\rho^{-1})\rho \in F^*(G)$. Therefore we may assume $f_0 = f$. However this implies that σ induces 1 on N as σ and $\sigma\rho^{-1}$ agree on M_0. Thus $H = \langle\sigma\rangle \times T$. This is impossible as $\sigma \notin O_p(H)$. Therefore we may assume that $[\sigma, E(G)] = 1$. Since τ is a conjugate of σ and $E(G)$ is a normal subgroup of G, the above argument

shows that we may also assume $[\tau, E(G)] = 1$. Hence $[H, E(G)] = 1$. For $i = 1,..., t$ let $T_i = Te_i$. By (2.2), $T_i = H_i \cong SL(2, A(\mu_i, \alpha_i))$, $i = 1,..., t$. These isomorphisms are given by $\sigma e_i = R(I)$ and $\tau e_i = R(a_{\mu_i}(\alpha_i))$. Let $A_i = A(\mu_i, \alpha_i)$, R_i the radical of $A(\mu_i, \alpha_i)$ and F_i the set of p^ath power of elements of $A(\mu_i, \alpha_i)$ where $p^a \geqslant \max\{\text{parts of } \mu_i\}$. Thus $F_i \cong GF(\alpha_i)$.

Let $P_i(1) = \{g \in SL(2, A_i) \mid g = I + g_1$, where g_1 is a 2 by 2 matrix over $R_i\}$. Since $A_i = R_i \oplus F_i$, $SL(2, A_i) = SL(2, F_i)\, P_i(1)$. Let $S_i = SL(2, F_i)$. Then $\sigma e_i \in S_i$. Suppose $P_i(1) \neq 1$. There is a conjugate ξ of σe_i in S_i such that $\langle \sigma e_i, \xi \rangle$ is not a p-group. Let $\xi = (\sigma e_i)^{s_i}$ where $s_i \in S_i$ and let $s \in H$ such that $se_i = s_i$. Then $\langle \sigma, \sigma^s \rangle$ is not a p-group and $(\langle \sigma, \sigma^s \rangle)e_i = \langle \sigma e_i, \xi \rangle \neq T_i$. This contradicts the minimality of H. Hence $P_i(1) = 1$ and $T_i = SL(2, F_i)$ for $i = 1,..., t$. The above argument actually shows that we may assume $T_i = SL(2, F_i) \cong SL(2, p)$. Therefore we may assume that $t = 1$ and $T \cong SL(2, p)$. If $M_0 \neq 0$, then $T = \langle \sigma_1, \tau_1 \rangle$, where $\sigma_1 = \sigma e_1$ and $\tau e_1 = \tau_1$. Since T induces 1 on M_0, $\sigma_1, \tau_1 \in Q_{f_0}$ with $f_0 < f$. Hence $T \leqslant F^*(G)$ by induction. As before we can infer $\sigma \in F^*(G)$ in this case. Therefore we may assume that $M_0 = 0$. Hence $H = T \cong SL(2, p)$ and the involution i of H induces -1 on M. Since G acts faithfully on M, i belongs to the center of G. Let $V = \Omega_1(O_p(G))/\Phi(\Omega_1(O_p(G))$, where $\Phi(\Omega_1(O_p(G))$ is the Frattini subgroup of $\Omega_1(O_p(G))$. Theorem 3.3 implies that every element of order p has minimal polynomial dividing $(X - 1)^2$ as linear transformation on V. However i centralizes V. Since $PSL(2, p)$ is p-stable [5, Theorem 8.4, p. 109], H must centralizes V. Hence every p'-element of H centraliezes $\Omega_1(O_p(G))$ by Burnside's theorem [5, Theorem 1.4, p. 174]. Since p is odd, every p'element of H centralizes $O_p(G)$ [5, Theorem 3.10, p. 184]. Therefore H centralizes $O_p(G)$ as H is generated by its p'-elements. Hence H centralizes $F^*(G)$ by Lemma 2.9. Thus by Lemma 2.10 we see that $H \leqslant F^*(G)$ and so $\sigma \in F^*(G)$, which contradicts our assumption $\sigma \notin F^*(G)$. This contradiction shows that $\sigma \in F^*(G)$. Therefore $G = F^*(G)$ as desired.

Suppose $O_p(G) \leqslant E(G)$. Applying induction on $|G|$ we see that every component of $E(G)$ has the required structure and Theorem 3.3 shows that $O_p(G)$ also has the required structure. We may assume without loss of generality that $O_p(G) \leqslant E(G)$ and G is quasi-simple. Thus $O_p(G) \leqslant Z(G)$. Let W be a nontrivial irreducible module of G in M and let G_1 be the group of automorphism induced by G on W. Then (G_1, W) is a quadratic pair for p in the sense of [9] such that G_1 is quasi-simple. Now the Main Theorem of [9] implies that $G_1/Z(G_1) = \bar{G}_1$ is isomorphic to one of the groups listed in the statement of that theorem. Since $p \geqslant 5$, the Schur multiplier of $\bar{G}_1$ is a p'-group (see for example [1] or [6]). Therefore $O_p(G) = 1$. Since G is quasi-simple, Theorem 4.2 implies that G is isomorphic to $SL(2, p^a)$ for some positive integer a. The proof of Theorem A is complete.

We now make some remarks concerning the case $p = 3$. Under a definition similar to that for $p = 3$ if $3 < |X|$ for $X \in \Sigma$, then using methods in [11], we can show that Theorem B is still valid in this case. However in the case

$3 = |X|$, example shows that the group $SL(2, 3) \times Z_3$ has a faithful module which satisfies all the assumption of Theorem B. Also in generalizing Theorem 2.11 and Theorem A, the fact that $SL(2, 3)$ is not perfect and is not generated by its 3′-elements causes trouble.

Finally it might be worthwhile to point out that in the conclusion (1) of Theorem B, G in general is not itself a member of Σ.

References

1. W. Feit, The current situation in the theory of finite simple groups, *in* "Proceedings of the 1970 International Congress of Mathematicians."
2. G. Glauberman, A sufficient condition for p-stability, *Proc. London Math. Soc (3)* **25** (1972), 253–287.
3. G. Glauberman, Quadratic elements in unipotent linear groups, *J. Algebra* **20** (1972), 637–654.
4. D. Goldschmidt, 2-Fusion in finite groups, *Ann. of Math.* **99** (1974), 70–117.
5. D. Gorenstein, "Finite groups," Harper & Row, New York, 1968.
6. R. Griess, Jr., Schur multiplitiers of the known finite simple groups, *Bull. Amer. Math. Soc.* **78** (1972), 68–71.
7. M. Hall, Jr., "The theory of groups," Macmillan Co., New York, 1959.
8. P. Hall and G. Higman, On the p-length of a p-soluble group, *Proc. London Math. Soc. (3)* **7** (1956), 1–42.
9. C. Y. Ho, Chevalley groups of odd characteristic as quadratic pairs, *J. Algebra* **41** (1976), 202–211.
10. C. Y. Ho, Quadratic pairs for odd primes, *Bull. Amer. Math. Soc.* **82** (1976), 941–943.
11. C. Y. Ho, Quadratic pair for 3 whose root group has order greater than 3, I, *Comm. in Algebra* **3** (1975), 961–1029.
12. C. Y. Ho, Linear transformation and collineation of finite translation planes, preprint 113, Mathematics Department, University of Brasília.
13. J. G. Thompson, Quadratic pairs, unpublished.